California Office of Health and Information Integrity

UPDATED INFORMATIVE DIGEST

Final Regulations for Demonstration Projects for the Electronic Exchange of Health Information

February 10, 2012

California Health and Safety (H&S) Code § 130277, authorizes the Director of the California Office of Health Information Integrity (CalOHII) to adopt regulations applicable to demonstration projects regarding health information exchange services.

Assembly Bill 278 (Stat. 2010 Ch. 227 (Monning), codified at Health and Safety Code § 130275 et seq.), authorizes the Director of CalOHII to approve demonstration projects for electronic exchange of health information. These projects evaluate policies and rules to better inform and serve the State and healthcare stakeholders while the infrastructure for the electronic exchange of health information is being developed. The demonstration projects will determine best practices to protect privacy in accordance with State and Federal laws while enabling electronic exchange of health information.

FINAL STATEMENT OF REASONS AND RESPONSE TO COMMENTS

California H & S Code § 130278 (b) exempts CalOHII from the rulemaking requirements of Section 11343.4 and Article 5 (commencing with Section 11346) and Article 6 (commencing with Section 11349) of Chapter 3.5 of Part 1 of Division 3 of Title 2 of the Government Code.

To ensure discussion and input on the demonstration projects regulations, CalOHII invited public comments on the initial proposed demonstration projects regulations in accordance with H & S Code § 11346 (b):

> "An agency that is considering adopting, amending, or repealing a regulation may consult with interested persons before initiating regulatory action pursuant to this article."

Public comments to the proposed demonstration projects regulations initiated substantive revisions to the regulations. In response CalOHII invited another round of public comments. After further review, research, and analysis of the

second round, it was concluded that public comments on these regulations had been addressed.

I. Section 126010: Applicability

These regulations are applicable to the Demonstration Projects Participants for the purposes of testing privacy and security policies and standards for the electronic exchange of health information.

CalOHII received comments concerning the use of “Applicant” and “Participant” referenced throughout the regulations, as well as the use of more general requirements where an applicable party is not identified. To address the confusion of terms, the regulations have been revised to identify the applicable entity in each provision.

II. Section 126020: Definitions

Several comments acknowledged acceptance of the use of unmodified, federally defined terms. Some terms, however, present conflicts due to inconsistencies in state and federal terms and definitions. Of the terms that were commented upon, three have been revised, two have been deleted, and four have had no change.

The modifications to definitions are as follows:

“Affiliated entity” – Revised

Since the term “entity” was removed from the definitions, in order to remain consistent , this term should also be removed from the term “affiliated entity”. “Entity” has now been replaced with “organization” to revise as “affiliated entity”. Also, as suggested by comments, the definition of this term is being revised to incorporate Organized Health Care Arrangements as defined by HIPAA.

Definition has been revised as follows:

> *(b) “Affiliated Organization” means legally separate organizations which have designated themselves as a single, affiliated organization and are under common ownership or control or are a part of the same Organized Health Care Arrangement (“OHCA”) as defined by HIPAA.*

“Authorization” – Revised

Comments had suggested the removal of the term. However, after careful review the term was maintained but the definition revised in order to provide

distinction of uses between “Authorization” and “Consent. We decided this would be necessary since HIPAA does not have a definition for “authorization” in its privacy rules, but has rules for uses and disclosures when an authorization is required. Insurance Code section 791.06 does not provide a definition of “Authorization”, but it utilizes the term when describing disclosure of personal or privileged information about an individual to the insurance institution, agent, or insurance-support organization. Civil Code section 56.05 defines authorization as:

> “56.05. For purposes of this part:
> (a) "Authorization" means permission granted in accordance with Section 56.11 or 56.21 for the disclosure of medical information”.

Section 56.11, referenced in Section 56.05, prescribes the requirement for obtaining authorization in certain settings but does not provide a definition of “Authorization”. Similarly, Section 56.21 does not provide a definition for “Authorization”, but provides specificities for which a valid authorization shall meet.

“Business Associate Agreement” – Deleted

One commenter noted that the definition for “Business Associate Agreement” in the regulations is more stringent than what is required in the provisions of HIPAA for business associates. It was suggested that CalOHII is trying to address some of the deficiencies of the HIPAA Privacy rule by creating a stringent definition and that by definition alone it would not suffice for policy purposes.

Creating a definition of “Business Associate Agreement” that contains stronger language than HIPAA does not provide for a more stringent policy for business associates and their agreements with covered entities. To create such a requirement in the regulations, Demonstration Project Participants would force change in the business associate agreement language in contracts for all of their business associates. The impact to Demonstration Project Participants would be labor and time intensive and would impede demonstration projects from moving forward. Therefore, the definition of “Business Associate Agreement” is removed from the regulations and relies on the HIPAA provisions for Business Associates as stated in the definition.

It should be pointed out that it is acknowledged through previous work of the California Privacy and Security Advisory Board (CalPSAB) that Business Associate Agreement language and requirements are insufficient and work remains to be done. The Privacy Steering Team has included this issue in their list of priorities for 2012 law harmonization work. Future iterations of the demonstration project regulation may include provisions that tighten Business Associate Agreement language and requirements.

“CMIA Provider” – No Change

As stated previously, this term is one of the terms added as a starting point in creating clearer terminology, and we will obtain feedback through the demonstration projects as to its usefulness and effectiveness. It is maintained that the CMIA limits the types of entities that can use and disclose medical information and is more restrictive by obligating non-provider entities to obtain an authorization to disclose IHI that was previously created, received, or derived from a CMIA provider or a health care service plan. Such increase of privacy protections under the CMIA makes California law more stringent than the HIPAA Federal law. In order to clarify this difference in state and federal laws the term “CMIA Provider” was created.

“EHR Vendor Agreement” – Deleted

Several commenters stated that the collection of EHR Vendor Agreements for transparency purposes was not the appropriate approach and mostly an administrative burden to the Participant and to CalOHII. These agreements are voluminous and include mostly technical specifications that CalOHII does not wish to review as part of the transparency process. Also, in light of the requirements of Section126040, revised per a comment we received, the EHR requirement is redundant since as a vendor with a business associate relationship with the provider, the EHR vendor will have a business associate agreement (BAA), and CalOHII in its own discretion may require copies of the BAAs. Therefore, the CalOHII has removed the EHR Vendor Agreement requirement from these demonstration projects regulations. CalOHII had intended to review EHR Vendor Agreements as documentation that highlights areas where uses and disclosures occur. However, since the collection and evaluation of EHR Vendor Agreements would be overly burdensome, the definition, as well as the provision to collect copies of EHR Vendor Agreements (§126040(b)(2)), have been removed from the demonstration projects regulations. At this time, the other provisions, including the collection of Participant Agreements and information regarding business associates are sufficient for the transparency provisions. Additionally, if and when a demonstration project participant is an HIO, there is no direct relation between the Participant and the EHR vendor.

Delete “Health Information Exchange” (HIE) – No Change

One commenter stated that the term “HIE” is a highly recognized term in the health care industry and that it would behoove CalOHII to keep the term in the regulations. Although we understand the commenter’s reasoning behind keeping the term “HIE”, the confusion of this definition, as well as the lack of clarity in any federal or local definition, has led CalOHII to remove this term. It does not assist in providing clear rules for the Demonstration Project Participants. For purposes

of these regulations, all health information that is exchanged electronically is referenced as disclosures of individual health information through an HIO, affiliated organization, or independent directed exchange.

“Health Information Organization (HIO)” – No Change

One commenter stated that the definition of HIO does not distinguish between those exchanges that merely oversee or govern exchanges and do not access and maintain identifiable health information versus those HIOs who do access and maintain the information and are exchanges which raise the most concern from a privacy and security standpoint. The definitions should clearly distinguish between those types of exchange arrangements that increase privacy risk to individuals and those that do not.

When measuring risk exposure, best practices dictate that organizations consider threats an asset may face as well as vulnerabilities the organization may have with respect to a particular threat. Based on this premise, CalOHII disagrees with the comment that organizations that do not actively access or maintain identifiable health information do not raise additional privacy risk. As long as there is the possibility of accessing the data (regardless of by whom) while it is in the possession of the HIO, there is an inherent risk that the data may be compromised. Ultimately, any time data is stored by or transmitted (data in-rest or data in-transition) through an organization, the possibility of unauthorized access is introduced which creates risk for that organization.

“Individual Health Information” (IHI) – No Change

One commenter suggested we use the term “medical information” as defined in the CMIA. As stated in the last iteration of the Statement of Reason, “medical information” under Civil Code section 56.05 is a difficult term to harmonize with the similar terms of “health information”, “individually identifiable health information (IIHI)” and “protected health information” under HIPAA. The term “individual health information” (IHI) has been drafted because the existing definitions mentioned above are irreconcilable. To use any of the existing terms would have allowed a gap in coverage of one of the laws and to use one of the common terms with a different definition would cause only further confusion on a very significant and critical element. Continued use of the term IHI is necessary to define the information protected in the demonstration project regulations and encompass the rules of both HIPAA and the CMIA.

“Participant” – Revised

One commenter suggested the removal “health care provider” from the definition of “Participant”. Due to the variety of policy that the demonstration projects will be testing, we are not limited to any one kind of entity or organization. For example, there may be a small provider that tests a tool to gauge their privacy

and security compliance as part of a risk assessment that they are required to do for meaningful use, as well as a requirement to comply with the HIPAA Security Rule. Thus, a small health care provider could very well be a demonstration project Participant.

Also, included in the term "health care provider" are hospitals and Integrated Delivery Systems (IDS). Omission of these types of health care providers from becoming Participants in the demonstration projects is not suggested as many of them are currently participating in the electronic exchange of health information. Therefore, the definition of "Participant" is retained in order to maintain the diversity of prospective participants for the demonstration projects.

However, the term has been revised to differentiate between a participant in the demonstration project and all other participants in a HIO by revising the term from "Participant" to "Demonstration Project Participant".

"Sensitive health information" – Revised

A few commenters stated that the definition of "sensitive health information" was too broad and did not adhere to the current legal requirements for certain types of health information. CalOHII agrees that the definition is broad and the usage of "traditionally recognized" stands subject to wide interpretations in the absence of a specified recommendation by the National Committee of Vital and Health Statistics (NCVHS) on what constitutes "traditionally recognized" sensitive health information. In its letter of February 20, 2008, to the Secretary of the U.S. Department of Health and Human Services, the NCVHS refers to a list of some categories of health information which NCVHS considers as "commonly considered" to contain sensitive health information, but it does not provide a definition for "commonly considered". Therefore, CalOHII has revised the definition to remain within the current legal framework. At the same time, CalOHII acknowledges, as does the federal government and other health care industry stakeholders, that there are issues that remain with the ambiguous definition of "sensitive health information" and that the ambiguity can lead to mistrust in an electronic health information exchange system.

CalOHII will be working with our Demonstration Project Participants and Privacy Steering Team members to further discuss this issue. Future iterations of the demonstration project regulations may contain a more refined definition of "sensitive health information".

The definition has been revised as follows:

> *"Sensitive health information" means legally established categories of sensitive information, such as genetic information, mental health, substance abuse treatment, HIV-related information, sexuality*

and reproductive health or specific segments of a patient's individual health information for which a patient has requested protection from disclosure in writing.

§126030 California Health Information Exchange Practices Principles

The principles in section 126030 were created and discussed through a publically vetted process, recommended through the stakeholders' structure to the Secretary of Health and Human Services in 2009, and approved by the Secretary. Additionally, the provisions of this section are aligned with California Civil Code § 56.07 following the principle of the more stringent law. The adoption of those principles as the demonstration project fair information practices for the electronic exchange of health information is maintained without change.

Some commenters expressed concern over section §126030 (a)(3)(C) which states:

"Challenge the accuracy of their individual health information and, if successful, to have the individual health information corrected, completed, or amended."

Commenters suggested that this language takes the provider's or organization's rights as caretaker of the data away. CalOHII disagrees because this section does not cause any issues with providers' or organizations' rights and responsibilities to be caretakers of the individual health information that they collect and use to care for a patient. This section of the principles is stating that a patient/individual has the right to challenge the accuracy. This same right is given by HIPAA which provides an individual with the opportunity to request amendment of his/her health record. This does not mean that a provider or organization must change the record to accommodate the request. It means that a provider or organization must review the request or challenge and make the proper amendments, only if necessary. There are very specific rules to amend health information per HIPAA 45 C.F.R. §164.526 and those rules do not compromise a provider's ability to use, rely, and keep record of the data.

§126040 Transparency and Complaint Process

Numerous comments were received regarding the collection of EHR Vendor Agreements as part of the transparency provisions. Comments suggested that the EHR Vendor Agreement may not be the appropriate documentation to collect for purposes of transparency in the demonstration projects. One commenter noted that these agreements can be hundreds or thousands of pages long and include mainly technical specifications rather than information that would be informative to the demonstration project. Several commenters suggested that the requirement should be to collect specific provisions that apply to health

information exchange only from the EHR Vendor Agreement. One commenter stated that since the requirement was based on anecdotal allegations that cannot be substantiated that the requirement be removed. Commenters unanimously agreed that the requirement would be an administrative burden that will adversely impact participation in the demonstration projects for the electronic exchange of health information.

The EHR Vendor Agreement poses administrative burdens on both the Demonstration Project Participant and the CalOHII staff and have therefore removed the requirement from the regulations. The collection of the EHR Vendor Agreement may not be necessary to meet the needs for transparency. At this time, the collection of Participant Agreements and information regarding BAAs are sufficient regulatory requirements to meet the need for observing the uses and disclosures of health information in an exchange scenario.

CalOHII also received comments suggesting that the various transparency provisions were administratively burdensome and would doubtfully become an industry requirement. To clarify, CalOHII is not requesting a copy of all of the Demonstration Project Participant's business associate agreements (BAAs). A general listing of business associate names and functions is requested because it is a simple way that sheds light on the uses and disclosures occurring under the guise of "health care operations" where the patients are unaware of when and if a treatment relationship has been applicable. This information is not trivial as it is a cornerstone to building trust in an electronic exchange system that will ultimately succeed in California – a trust relationship which includes all parties involved. Likewise, the HIE Participant Agreements will demonstrate the premises in which electronic exchange happens, including members of the exchange and the rules by which they exchange health information. Although seemingly burdensome, these transparency pieces will fortify trust in an exchange system.

One commenter noted that the requirements for the Notice of Privacy Practices (NPP) and complaint process in the regulations would not apply to an HIO. A Demonstration Project Participant who is an HIO would not be supplying NPP's to a patient or obtaining complaints directly from patients. The provisions for NPP and complaint process have been revised to make clear the requirements for particular types of Demonstration Project Participants.

§126042 Trade Secret Designation and Protections

One commenter was concerned that the provisions regarding trade secrets contravene the Public Records Act. The application of trade secret protections must be determined first by whether the material in the application meets the definition of a "trade secret" (as defined by the Uniform Trade Secrets Act (Civil Code section 3426.1). Therefore, any material provided to the Agency (CalOHII)

is not determined as a “Trade Secret” based on the Agency’s determination that it is a trade secret, but that it must meet the definition of a trade secret in accordance to the Uniform Trade Secrets Act. In doing so, if any material submitted by an Applicant does not meet the definition, then it should be treated as material subject to the provisions of the Public Records Act.

CalOHII disagrees with the comment that “Contrary to proposed section 126042 (a) (1), the Public Record Act does not permit an agency instead to make the record “exempt from disclosure under the Public Records Act during the time the records are in the possession” of the agency.” The Agency (CalOHII) is supported by law to determine if proposed information is a trade secret or not in accordance to Government Code 6254 (Note: Specifically sections 6254 (k) and (q) are supportive).

The regulations have been revised as follow:

> *“After review, if CalOHII determines that the material submitted meets the definition of a “trade secret”, then CalOHII will treat the material as such and will exempt it from disclosure. If it is determined that the material does not meet the definition of a “trade secret”, then the material or information will be disclosed as public information in accordance with the Public Records Act, Government Code section 6250.”*

§126050 Permitted Purposes for Exchanging Health Information

CalOHII received comments that the regulations only apply to initial electronic disclosures and do not cover the secondary uses and disclosures of health information. While the needs and issues surrounding secondary uses and disclosures of health information are understood, we are not at a point where we can set clear policy through regulation. The Federal government, as well as California’s stakeholder groups through CalOHII, is working on the secondary use and disclosure policy issue. CalOHII will be following the work of the Federal government closely; for example, the Office of the National Coordinator for Health IT is currently testing the use of certain metadata standards in pilots with Indiana and Montana through the state health information exchange program. Future iterations of the demonstration project regulations that will test policy for secondary uses and disclosures of health information.

As stated in the DAR provisions of the regulations, a Demonstration Project Participant may request to test alternative policies that are more protective of health information. This would allow Demonstration Project Participants to test more stringent policy and the accompanying technology that would protect individual’s health information. Any entity or organization that can test stronger

privacy protections through specific secondary use and disclosure policy and technology is encouraged to participate in the demonstration projects.

Another commenter stated that section 126050(c) is problematic in that it appears to omit fax and email exchange from protections. To clarify, the intent was not to release exchanges using email and electronic faxes from the requirements of the HIPAA Security Rules. Indeed, all Project Participants must abide by all HIPAA Security Rules and this would include protection of all electronic health information, including email and electronic fax regardless whether the exchange is for permitted uses or other business uses. Since the definition of an "independent directed exchange" would include any electronic transaction over the internet using encryption including emails and electronic faxes, CalOHII excluded electronic faxes and emails from the permitted purposes and permitted secondary purposes provisions as it did not want to impede current business practices that utilize electronic fax and email since these entities should already have these security measures in place. .

§126055 Informing and Consent; exceptions

Comments were received that the emergency access provision, also known as the break-the-glass provision, which prohibits providers' access to medical information in the event that a patient has explicitly denied consent, is a potentially harmful provision. While this is a concern, proper education in place an individual should be entitled to make the resolute decision to not participate in electronic exchange and that decision should be honored. This would include exclusion of emergency access. Providers may still obtain medical information in an emergency through other means such as phone and fax. This provision will be evaluated closely in the demonstration projects as to ascertain the impacts and viability of the provision.

One commenter stated that the regulations did not take into consideration the re-establishment of consent after it has been revoked. We revise the regulations to include re-establishment of consent.

One commenter stated that they believe the premise for the consent requirement is fundamentally wrong and that the CalPSAB never reached consensus for an opt-in policy. To clarify, in 2010 the Secretary of Health and Human Services asked the Board to reconvene and re-evaluate the consent policy recommendation for the opt-in model. The Board did so and at its meeting in December of 2010 by vote of its majority restated its patient opt-in consent policy and forwarded its decision to the CHHS secretary via a letter. Thus, the Board did reach consensus at that point for an opt-in policy. The January 2011 letter of CalPSAB to the CHHS secretary has been posted to CalOHII website.

Multiple comments were received opposing the requirement for consent for independent directed exchange. Commenters stated that conduit modes of exchange that do not require a Business Associate Agreement should be outside of the scope of the regulations. Commenters also stated that there are no additional downstream privacy or security risks to exchange of health information via independent directed exchange as defined by the regulations. The independent directed exchange does not carry the same risks as using a third party HIO and that HIOs may vary in their accessibility to health information; however, privacy risks still remain related to secondary uses and disclosures of health information. Additionally, in line with the provisions of H&S Code § 130279 (d)(1), this as an area critical to building consumer trust and confidence in the health information exchange system. It also will demonstrate how direct exchange can be done in a safe way. Therefore, the consent requirement for independent directed exchange remains in the regulations.

The DAR process will allow any Demonstration Project Participant who would like to demonstrate a more protective process that would not require consent for independent directed exchange to do so. This could entail strong secondary use and disclosure policy as well as technical safeguards that enforce that policy. The DAR requirements in section 126060(b)(3)(B) related to independent directed exchange will allow a multitude of entities who have implemented independent directed exchange to test alternative approaches including no consent.

For clarification purposes, §126050 Permitted Purposes for Exchanging Health Information was added a third type of electronic exchange of health information. Neither definition of HIO nor independent directed exchange include affiliated organizations such as organized health care arrangements (OHCA), independent physician associations (IPA), or integrated delivery systems (IDS). Our intent was not to exclude these organizations as Participants in the demonstration projects. These types of exchanges were included in the permitted purposes section of the regulation. Affiliated organizations are not included in the consent requirements as CalOHII is only requiring those entities that are unaffiliated to obtain consent.

One commenter suggested that the informing requirements be addressed in the Demonstration Project Participant's Notice of Privacy Practices (NPP). CalOHII disagrees that this would be sufficient to educate patients on the specific benefits and risks to using electronic exchange of health information. CalOHII retains the requirements for informing at section 126055.

CalOHII also received comments that the consent requirements outlined in the demonstration project regulations were inadequate and did not require providers or their staff to have conversations with patients nor did they require notice and consent to be presented in the patient's primary language. CalOHII retains the requirements for consent at a higher level in order to allow Participants to

demonstrate different ways to operationalize the consent requirements. Demonstration project regulations do not override any existing law that requires patient's be given documentation in their primary language. Those requirements will still need to be addressed by the Participant's in the demonstration projects.

One commenter stated concern regarding the concept of "centralized consent registry" and that it would take the consent process outside of the relationship between provider and patient. CalOHII does not see the consent process for the demonstration project as a one size fits all scenario. We are open to having different Participants test different ways of educating patients and obtaining consent. The consent registry is one part of a bigger picture that requires informing patients of their rights, benefits, and risks of participating in electronic exchange of health information. Opposing comments stated that a central consent management process will remove a considerable burden from small practice physicians and greatly improve participation in proposed projects. The anticipated outcome would be a well-balanced approach to the consent process using a variety of education tools and a variety of technological features that support the process.

A comment was received regarding the inadequacy of the consent provisions and that consent should not be compelled or used for discriminatory purposes and that consent should include full transparency and education. The demonstration project regulations will allow for a variety of ways to implement consent. CalOHII declines to define a specific strategy for consent and informing, but rather look to the demonstration project Participant's creativity to design a process that fulfills the needs for transparency and education.

Section 126050 details conservative requirements related to consent processes with a significant portion of the requirements being placed on the front-line providers of care. Further it is implied that the proposed consent requirements apply equally to all permitted purposes of use. The commenter stated there should be clarification for each previously-permitted purpose. CalOHII maintains the regulations as is in this regard since these demonstration projects are for testing privacy and security policies and standards, and the results will inform us as to the strengths and/or barriers.

§126060 Requests to Demonstrate Alternative Requirements

Various comments were received regarding who would be creating DARs. One set of commenters stated that Applicants would be responsible for creating DARs, while another set of commenters stated that CalOHII would be responsible for creating DARs. To clarify, the DAR process is meant to be the responsibility of the Applicant. General requirements in section 126060(a) are the written requirements for the Applicant to include in a DAR request to CalOHII. Section 126060(b) was written as factors that CalOHII will take into consideration

when evaluating the DAR. Those factors should be included in the DAR submission to CalOHII.

Multiple comments were received stating that the process for testing alternatives was unclear and the approach provides disincentives for the adoption of EHRs, and imposes a burden on both patient and providers. Comments stated that the regulations were intended to regulate the initial electronic disclosure of health information only and that downstream disclosures could only be addressed by the DAR process. In addition, the process itself was a disincentive to an entity actually testing an alternative. Commenters were concerned that the factors by which CalOHII would evaluate the DAR were difficult to meet. Further, that the DAR requirements would not be imposed on Demonstration Project Participants that use the core approach of these regulations and thus, implying it would appear to penalize those entities who chose to test alternatives. It was stated that this approach may cause disincentives to entities that might very well be able to test stronger privacy protections that do not include consent. Commenters urged the State to draft more broadly applicable regulations that will allow for alternative requirements to be more easily tested. The DAR requirements have been modified in order to alleviate the requirements by which CalOHII would evaluate the DAR. However, it is maintained that the DAR is to allow for testing new technologies and applications that enable the transmission of protected health information, while increasing privacy protections by ensuring only required health information is transmitted for purposes and uses consistent with State and Federal law.

One commenter was concerned with the uncertainty of the timeframe given in section 126060(c) regarding CalOHII's approval process for the demonstration projects. The commenter requested a specific timeframe such as '30' or '45' days. CalOHII acknowledges that a set timeframe will prevent delay in moving forward with the demonstration projects. The regulations are revised provide a 45 day turnaround for CalOHII to review and approve any requests for DAR. Also revised in the regulations is a 15 day extension for CalOHII in the case that a DAR is submitted with insufficient information to determine approval. This time will allow CalOHII to follow up with the Applicant and collect the necessary information and documentation.

One commenter stated that it was not clear in the regulations whether an Applicant who was approved as a Demonstration Project Participant would be permitted to perform services that were not covered by the permitted purposes and were not approved by a DAR process. CalOHII acknowledged the comment, and language is added to clarify that a Demonstration Project Participant would be permitted to perform services that are not covered by the permitted purposes and/or the DAR process so long as those services are consistent with State and Federal law. Also, this provision is redundant to the section 126040(b)(4) for those situations where possible continued access to IHI would be covered by BAAs which can be obtained by CalOHII.

A comment was received regarding the use of de-identified information that should be prohibited in the demonstration projects until clear policies are promulgated. Neither the State nor the Federal government has promulgated clear policies regarding the appropriate use of de-identified data. The Privacy Steering Team is addressing this issue as one of its priorities for 2011-2012. CalOHII is not able to add any regulatory language associated with de-identification of health information at this time. Future iterations of the demonstration project regulations may include such language.

One comment was received that stated that section 126060(b)(3)(B)(iv) appears to create higher standards of handling sensitive health information. We agree that the definition in section 126020, as well as section 126060(b)(3)(B)(iv) create a more ambiguous set of rules for sensitive health information then what currently exists in law. The definition and this section are revised to make the demonstration project regulations consistent with existing law. Please see section 126020 for discussion regarding the definition of "sensitive health information".

One commenter stated concern over section 126060(b)(3)(B)(vi) as it specifies no re-purposing or re-directing of information by the system vendor. This provision applies to more than just system vendors and is revised as follows:

> *(vi) There is no re-purposing or re-directing of the information.*

After careful and diligent review of the DAR requirements and the public comments, sections of the DAR have been removed because the requirements could be covered in the memorandums of understanding that are drafted and negotiated with each Demonstration Project Participant based on their specific structure and activity in the field of the electronic exchange of health information.

§126070 Security Requirements - General

One comment was received related to the general security requirements. This commenter suggested alternatives to the use of the word "ensure" where the regulation seeks to require organizations to protect IHI. This commenter felt the use of the word "ensure" implied the requirement for a guarantee of 100% compliance which the commenter felt was infeasible. The use of the term "ensure" is infeasible and have therefore changed this section of the regulations to alleviate this issue. It was deemed that changing the term "ensure" to "protect" and "monitor" were more tangible tasks to achieve while still maintaining the original intent of the regulations. Also, CalOHII's intent was to avoid being overly prescriptive for the speed with which technology is evolving, and to ascertain the challenges faced by the participants in carrying out these

mandates. These regulations are meant to be evolving as results of the demonstration projects are assessed, and could be amended in the future.

§126074 Security Requirements – Physical Controls

One comment was received related to physical controls. This commenter stated that many of the security requirements in §126074[1] that deal with safeguards for storing data apply to all Demonstration Project Participants even though some may not actually store IHI. CalOHII agrees that in rare cases these requirements may not apply to all organizations. Accordingly, the regulation text is modified to apply to organizations that store data.

§126076 Security Requirements – Technical Controls

One comment was received related to technical controls. This commenter suggested making clear the requirement that only secure methods of email are permissible for sharing IHI. CalOHII agrees and has modified the language in this section to indicate that encryption or an equivalent mechanism must be used in email and other messaging transmissions containing IHI.

§126090 Demonstration Projects Oversight

This section of the regulations did not receive any comments from the public and will remain as written.

General Comments

One commenter stated that the uses of the term “personal representative” in the regulations were used in a manner that does not distinguish the specific rights of an “individual” and the “personal representative” which are not identical in nature. In an effort to remove the slightest ambiguity, we have added “legally authorized” to account for the fact and emphasize that a “personal representative” means the person who has the legal authority to act on behalf of the individual, under authority of a power of attorney, or due to incompetency, or infancy of the principal party.

[1] The commenter erroneously referenced §126070 instead of §126074 when discussing concerns relating to safeguarding stored data. Accordingly, this comment us addressed as it applies to §126074.